BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-114

30 JUNE 1994

AIR FORCE MATERIEL COMMAND
Supplement 1

27 NOVEMBER 1996

Communications

SOFTWARE MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFC4A/XPSP
(Capt Joe L. Mattingly)
Supersedes AFR 700-26, 15 December 1988, and
AFR 700-9, Volume 1, Attachment 4,
15 March 1985.

Certified by: HQ USAF/SC
(Lt General Carl G. O'Berry)
Pages: 53
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*. It also incorporates procedures outlined in Department of Defense (DoD) Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988; and DoD Instruction 5000.2, *Defense Acquisition Management Policies and Procedures*, February 23, 1991. It identifies responsibilities for managing, developing, maintaining, and implementing Air Force computer software. Refer technical questions on the content of this instruction to Headquarters, Air Force Command, Control, Communications, and Computer Agency (HQ AFC4A), Directorate of Plans and Analysis, Software Processes and Strategies Division (XPS), 203 W. Losey Street, Room 1065, Scott AFB IL 62225-5224. Refer recommended changes and conflicts between this and other publications to HQ AFC4A, Policy and Procedures Branch (XPXP), 203 W. Losey Street, Room 1065, Scott AFB IL 62225-5224 using AF Form 847, **Recommendation for Change of Publication**. For a listing of references, abbreviations, acronyms, and terms, see **Attachment 1**.

(AFMC) This supplement does not apply to the Air National Guard or US Air Force Reserve units and members. This supplement contains guidance and procedures for management of small computer software within AFMC. Procedures and guidance for the management of software controlled by AFMC are the responsibility of central design activities (CDA). The AFMC CDAs are the Materiel Systems Group (MSG), Standard Systems Group (SSG), and the 38th Engineering and Installation Wing (38 EIW). The CDAs will forward a copy of any such guidance to HQ AFMC/SCDP, 4225 Logistics Avenue, Suite 6, Wright-Patterson AFB OH 45433-5745. Local supplements can add to but not take away from the AFI and major command supplements.

AFI 33-114, 30 June 1994, is supplemented as follows:

SUMMARY OF REVISIONS

This is the initial publication of Air Force Instruction (AFI) 33-114. It revises paragraph 2-8 and 2-20 through 2-23 of Air Force Regulation (AFR) 700-26. It also incorporates paragraph 2-4, 2-14, and AFR 700-9, Volume 1, attachment 4 .

(AFMC) This publication is made necessary due to the addition of the Data System Designators (DSDs) process at paragraph 5.2.4.

Section AIntroduction2

1.Purpose. 2

2.Objectives. 2

Section BManaging Computer Software2

3.Purpose. 2

Section CSoftware Development12

4.General Requirements. 12

Section DSupport23

5.General Requirements. 23

Section EResponsibilities27

6.HQ USAF/SC: 27

7.Secretary of the Air Force for Acquisition (SAF/AQ): 27

8.Major Commands: 27

9.Major Command Small Computer Technical Centers (SCTC): 28

10.Headquarters, Air Force Command, Control, Communications, and Computer Agency: 29

11.Implementing Commands: 29

12.Supporting Commands: 29

13.Operating (Using) Commands: 30

14.Other Participating Organizations: 31

15.The Computer Resources Working Group: 31

Attachment 1—GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS 33

Attachment 2—KEY ORGANIZATIONS 41

Attachment 3—AIR FORCE STANDARD PROGRAMMING LANGUAGES 42

Section A—Introduction

1. Purpose. This instruction outlines procedures for software personnel to plan, develop, use, and support C4 systems to effectively and efficiently complete their assigned missions.

2. Objectives. This instruction:

- Gives commanders, managers, and software developers at all levels specific guidelines for managing C4 software.
- Outlines requirements for standardizing documentation, quality assurance procedures, and implementation processes.

- Gives methods for maximizing operational effectiveness and minimizing costs.
- Gives methods for enhancing system performance, maintainability, interoperability, portability, reliability, security, and availability of systems.
- Gives methods for developing computer technology and support systems by introducing modern software engineering principles and management practices.

Section B—Managing Computer Software

3. Purpose. This section explains how to manage computer software and refers readers to other instructions when necessary.

3.1. Early Program Documentation. Early program documentation will address basic management, support, and requirements of systems.

3.1.1. Mission Need Statements (MNS). For systems that are likely to include computer software, address the following type questions, and include the answers in the MNS (see AFI 10-601, *Mission Needs and Operational Requirements Guidance and Procedures*):

- Is there a need to operate the software on different systems?
- Will the software be used jointly, with a host nation, or Air Force only?
- Have projected changes in, and growth of requirements been considered and/or addressed?
- What requirements are there for security?
- What are the other anticipated support requirements?
- What maintenance requirements are there for keeping equipment running reliably?
- Will additional manpower positions be needed to support the system?
- Are new facilities required to operate and maintain the equipment and the software?

3.1.2. Preliminary System Operations Concept (PSOC), System Operations Concept (SOC), and Operational Requirements Document (ORD). The PSOC, SOC, and ORD define the role of computer software and explain how to access support services.

- Show what type of specific computer support services is needed and how commands will access it.
- Identify a preferred support concept that complements other portions of the SOC.
- Develop and document a Security Concept of Operations as part of, or in addition to, the PSOC and SOC.

3.2. Architecture.

3.2.1. AFI 33-102, *C4 Systems Long Range Planning,* provides policy guidelines for planning, developing, and maintaining functional, data, and physical models and architectures.

3.2.2. Use these pamphlets for planning and developing software with a life-cycle of more than two years:

- Air Force Pamphlet (AFP) 700-50 (Volume 1, *Air Force Communications-Computer Systems Architecture Overview;* Volume 2, *Deployable Communications-Computer Systems*

Architecture; Volume 4, *Local Haul Information Transfer*; Volume 5, *Long-Haul Information Transfer*; Volume 6, *Integrated Systems Control*; and Volume 7, *Air Force Communications-Computer Systems Architecture Software Architecture)*, a multi-volume set of pamphlets, for current and future Air Force C4 architectures.

- AFP 700-50, Volume 1 specifically address computer software issues.

3.3. Security.

3.3.1. AFPD 33-2, *C4 Systems Security*, gives policy guidelines for developing and using the computer, communications, and TEMPEST security programs needed for all Air Force C4 systems. This policy directive provides the structure for implementing DoD Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988.

3.3.2. Air Force Index (AFIND) 5, *Specialized Communications-Computer Systems Security Publications*, lists Air Force systems security instructions (AFSSI) and memoranda (AFSSM) that give further direction and guidelines for security. Find information in this publication grouped according to security discipline.

3.4. Software Quality Evaluation.

3.4.1. Personnel define the scope of the software quality evaluation program for the software development life cycle.

3.4.1.1. To find requirements for establishing a software quality program, refer to DoD 2168-STD, *Defense System Software Quality Program*, (see Military Standard (MIL-STD)-499, *SUBJECT*, pending publication).

3.4.2. More than one organization, including an independent organization such as the Independent Verification and Validation (IV&V) program, or an operational testing organization, may evaluate computer software products and procedures.

3.4.3. Use metrics or other types of management indicators to monitor software development.

3.5. Configuration Management.

3.5.1. Define an overall approach for configuring computer systems according to MIL-STD-483A, *Configuration Management Practices.* Also see MIL-STD-973, *Configuration Management*, and AFR 14-1, *Configuration Management*, for further guidance.

3.5.2. The implementing, operating, and supporting commands will apply established management procedures to manage the configuration of computer products, maintain them in functioning order, and make sure they perform the tasks they were designed to do.

3.5.3. Organizations making changes to software will continue to evaluate product quality by monitoring the effects of software enhancements and modifications, the adequacy of software products, and personnel compliance with established procedures.

3.6. Reviews and Audits. Reviews and audits are conducted following MIL-STD-1521B *, Technical Reviews and Audits for Systems, Equipment, and Computer Software*.

3.6.1. System Design Review (SDR). Hold SDRs to formally assess the tasks the system needs to accomplish before proceeding with preliminary designs.

3.6.2. Software Development Reviews. The implementing agency will normally conduct these software development reviews:

- Software Specification Review.
- Preliminary Design Review.
- Critical Design Review.
- Test Readiness Review.
- Functional Configuration Audit.
- Physical Configuration Audit.
- Formal Qualification Review (FQR).

3.7. Data Management.

3.7.1. All Air Force organizations will follow the guidelines published in AFI 33-110, Air Force *Data Administration Program*, DoD 8320.1-M, *Data Administration Procedures,* September 26, 1991 , and DoD 8320.1-M-1, *Data Element Standardization Procedures,* January 1993.

3.7.2. C4 systems design documentation must incorporate standard data elements and their attributes.

3.8. IV&V.

3.8.1. Consider using IV&V when developing or modifying computer resources.

3.8.2. Based on recommendations of the computer resource working group (CRWG), the program manager will:

- Locate an organization that does IV&V.
- Determine the level at which personnel from the IV&V organization need to be part of the development effort and plan to include them.
- Document IV&V plans and decisions in the computer resource life cycle management plan (CRLCMP).

3.8.3. Operating and supporting commands will consider using each other to perform IV&V for systems for which they share support responsibility.

3.8.4. The implementing command will:

- Define and control communications between the IV&V agency and the development organization.
- Give the IV&V organization copies of development specifications, design documents, listings, and technical data.
- Resolve discrepancies found during IV&V. See AFP 800-45, *Software Independent Verification and Validation (IV&V),* for further guidance.

3.9. Commercial Software Guidance.

3.9.1. Commercial Off-the-Shelf (COTS) Computer Resources. COTS computer resources consist of the same computer software packages the vendor sells commercially. (*WARNING:* Vendors may decide to modify this software to suit themselves.) Commercial markets and independent contractors and vendors rather than the Air Force control design configurations of COTS

computer software. When a system includes COTS computer resources, the implementing command will:

- Include COTS deliverables in the logistics support analysis (LSA) and make sure the LSA addresses the support needs of COTS throughout the system's life cycle.
- Make sure the LSA supplies sufficient documentation for COTS computer resources for the life cycle of the system's operation. ***Note: Documentation need not adhere to military documentation standards.***
- Support COTS computer resources at the vendor's most recent revision level, unless upgrades would adversely affect systems operation.
- Negotiate competitively when buying support for COTS resources.

3.9.2. If an established contract logistics support approach for COTS exists, the implementing command will acquire the documentation and data rights, licensing, and subscription services that allow the Government to take over support of the system (such as options to purchase or escrow proprietary information), if necessary.

3.9.2.1. The supporting command will:

- Maintain up-to-date licensing and subscription services (such as vendor field change orders and software releases) throughout the life of the system. ***Note: Don't alter COTS resources as this may rule out contractor logistics support or void licensing or subscription services.***
- Provide logistics support and contracts out for subscription services required to update and maintain COTS assets.
- Evaluate operational and logistic impacts of changes due to subscription-related hardware and software upgrades.

3.9.2.2. The operating command will:

- Review proposed technical changes and work with the supporting command during upgrade and modification to COTS assets.
- Evaluate the impact of changes on deadlines and mission goals due to subscription-related software upgrades.

3.9.3. For Purchases of COTS Software:

- Consider site licensing when buying several copies of a software package.
- Consider software maintenance costs before buying. Some companies offer free or nominal fees for upgrades. ***Note: Before buying upgrades, make sure software is not already available.***
- For additional guidelines, refer to the Software Technology Support Center (STSC), Hill AFB UT.

3.9.4. The Air Force forbids the use of software acquired directly from non-DoD electronic bulletin boards, the public domain, or shareware sources. This software may contain hidden defects that can result in system failure or loss of data.

3.9.4.1. The Air Force allows the use of such software only after it is certified by a software testing facility, such as the Air Force Information Warfare Center (AFIWC), Kelly AFB TX,

the major command (MAJCOM) SCTC, or the Standard Systems Center (SSC/SSM) 85 Hodges Avenue South, Maxwell AFB - Gunter Annex AL 36114-6343.

3.9.4.2. Distribute approved software in a way that prevents tampering.

3.9.4.3. Make sure there are no copyright violations for COTS software used, and that all computer systems are free of "pirate" software.

3.9.5. (Added-AFMC) Guidance For the Use of Small Computer and Network Computer Server Software. Supervisors, or their designated representatives, will ensure that the following requirements are made known to all personnel and periodic audits are conducted to verify compliance with this guidance. This guidance should be disseminated by organizations (unit/2-letter) to all users of small computers.

3.9.5.1. (Added-AFMC) Install only commercial software, including shareware, that has been purchased through the government procurement process and which has been properly licensed on AFMC small computer systems.

3.9.5.2. (Added-AFMC) Follow all provisions of the licensing agreements issued with the software as modified by the Federal Acquisition regulations extracted in the procurement contract.

3.9.5.3. (Added-AFMC) Register organizational ownership of commercial software.

3.9.5.4. (Added-AFMC) Do not make illegal copies of copyrighted software. In other words, only make the number of copies stipulated in the applicable licensing agreement. If the license is for multiple users, do not exceed the authorized number of copies/users at any given time.

3.9.5.5. (Added-AFMC) The supervisor or designated representative will:

3.9.5.5.1. (Added-AFMC) Maintain records of installed software on each system.

3.9.5.5.2. (Added-AFMC) Maintain an inventory of all software (whether it is installed or not).

3.9.5.5.3. (Added-AFMC) Ensure that a license or other proof of legal use is available.

3.9.5.6. (Added-AFMC) Store evidence of license in a secure location, i.e., closed file cabinet, etc.

3.9.5.7. (Added-AFMC) Dispose of old versions of software when upgrades are purchased as stipulated in the applicable licensing agreement. Upgrades from the original software vendor are normally considered a continuation of the original license, not an additional license.

3.9.5.8. (Added-AFMC) Do not install copies of software for installation on an individual's home computer unless the licensing agreement permits users to do so. When software is installed on an individual's home computer system, use it only for government business. Personal utilization is normally a violation of the copyright law, and the individual will be held accountable and liable.

3.9.5.9. (Added-AFMC) The supervisor or the designated representative will audit the inventory of all software, annually, to ensure that no illegal copies of commercial or shareware software are installed or on hand. If there is evidence of criminal misconduct on a government small computer or network computer server, the supervisor should contact the Staff Judge Advocate's office for advice before taking any action. It is the responsibility of the organiza-

tional commander (2-letter) to establish procedures for the inspection of small computers and servers within the organization.

3.9.5.10. (Added-AFMC) When systems are declared surplus, delete all data files and software other than the operating system software. Delete the operating system software if it is not declared surplus with the computer system. Ensure approved overwrite procedures are followed.

3.9.5.11. (Added-AFMC) Do not install personally-owned software on government small computers and server systems unless authorized by the two-letter organizations, and the following guidance is followed:

3.9.5.11.1. (Added-AFMC) Request for Use. The individual wanting to use the software must justify, in writing, why the existing Air Force-owned software does not meet the need, and why the personally-owned software will satisfy the requirements; the time the software will be needed; and the name, version and serial number of the software. A copy of the software license and copyright agreement is to be attached to the requesting letter as well as the conversion plan outlined in 3.9.5.11.5.

3.9.5.11.2. (AFMC) Validation and Approval. Submit the letter to the requester's three letter organization for validation of the entire package (the request, reasons for the request, conversion plan, etc.). When validated by the three-letter organization, submit the package to the two-letter organization for approval. Anytime there is a change in personnel at the two-letter level, the new two letter must approve the package. If the two letter deems it appropriate to delegate this responsibility, this delegation is to be covered in an internal agreement. The same process, as detailed above, must be followed. Ensure local designated approval authority requirements are met for additional software.

3.9.5.11.3. (AFMC) Virus Check. All personally-owned software must be virus checked prior to installation on a government small computer. The requiring organization has authorization to virus check this software with an approved virus check program according to Air Force Systems Security Memorandum 5023, Viruses and Other Forms of Malicious Logic, dated 1 August 1996. Contact the base C4 systems security office for assistance.

3.9.5.11.4. (AFMC) Copyright/License Agreement Compliance. The individual requesting to use personally-owned software assumes all responsibility for complying with the software license and copyright laws. There will be no compensation for the government's use of personally-owned software.

3.9.5.11.5. (AFMC) Conversion Plan. The requester must prepare a conversion plan showing how the files they create with their personally-owned software can be converted for use with a comparable government software package.

3.9.5.11.6. (AFMC) Software Developed by Government Employees. Software that is developed by government employees and does not require a license, i.e., Air Force Institute of Technology, is authorized for use applying the same approval process identified in 3.9.11.2. Proof that the software was government-developed is to remain with the computer on which it resides. The software is to be virus checked according to 3.9.11.3.

3.9.5.11.7. (AFMC) Ownership. All files created with the personally-owned software are the property of the government. This software is to be used with unclassified data only.

3.9.5.11.8. (AFMC) Unauthorized Use of Personally-Owned Software. The personally-owned software will not be installed on a file server, local area network, or an office automation network. Any damages incurred as a result of the use of this type of software will be the responsibility of the individual.

3.9.5.11.9. (AFMC) Other. The using individual must keep the original documentation, original disks, a copy of the software license agreement, to include multi-user license agreements, and copyright agreement with the government small computer and server while the software resides on the system. A disk with a copy of the program and whatever documentation is available is acceptable for freeware and shareware.

3.10. Documentation.

3.10.1. Refer to DoD 2167A-STD, *Defense System Software Development*, and DoD 7935A-STD, *Defense System Software Development*, for:

- The standards used to develop and revise software documentation.
- Standards and descriptions for each of the technical documents produced during the life cycle of the software. DoD 2167A-STD is the preferred
- standard.

3.10.1.1. When DoD 2167A-STD does not provide the needed support, use DoD 7935A-STD. ***Note: MIL-STD-498 will replace DoD 2167A-STD and DoD 7935A-STD, when printed.***

3.10.1.2. Document and tailor all necessary data item descriptions associated with DoD 2167A-STD or Air Force AISs according to DoD 7935A-STD. See MIL-STD-498, pending publication.

3.10.1.3. Refer to:

- AFM 171-100 series publications (Volume 1, *Automated Data Systems {ADS} Standards*; Volume 2, *Automated Data Systems {ADS} Standards - H6000 Series ADS*; Volume 5, *Automated Data Systems {ADS} Series ADP*; Volume 6, *Development and Documentation of Automated Data Systems (ADS) - Small Computer*; and Volume 8, *Automated Data Systems {ADS} Standard Multiuser Small Computer Requirements Control {SMSCRC} System*) for information on how the Air Force implements DoD 7935A-STD and for additional documentation required for standard systems.
- AFM 171-100, Volume 1 for information on the minimal amount of documentation required for all computer programs and other software applications.

3.10.1.4. Prepare documentation having potential North Atlantic Treaty Organization (NATO) application according to NATO standardization agreements. Documents:

- Must support NATO rationalization, standardization, and operating requirements that enable the use of software on different systems (see AFI 60-103, *International Military Standardization Programs* {will supersede AFR 73-6, *North Atlantic Treaty Organization Military Agency for Standardization Coordinating Committee, and American-British-Canadian-Australian Armies Interational Military Standardization Programs,* when published).
- Must comply with nontreaty international standards.

3.10.1.5. For software documentation, give precedence to procedures that:

- Eliminate needless documentation by tailoring the amount of DIDs and how much they cover.
- Keep documentation requirements consistent with development methodologies. ***Note: Documentation requirements don't change even when personnel use rapid software prototypes, incremental software development techniques, and carefully considered software design methodologies.***
- Create data necessary for effective software support and maintenance by third-party or Air Force personnel over the system's operational life.

3.10.2. CRLCMP. The CRLCMP serves as the primary planning document for computer resources throughout the system life cycle. It complements the integrated logistics support plan (ILSP).

3.10.2.1. Operating and supporting commands will implement changes to their operating instructions, technical orders, and other directives in the CRLCMP.

3.10.2.2. CRLCMP:

- Begin development during the concept exploration phase according to DoD Instruction 5000.2/Air Force Supplement 1, *Defense Acquisition Management Policies and Procedures*, February 23, 1991, with Change 1
- Include updates as necessary to reflect changes in management decisions, in software planning, and in critical computer resources during deployment.
- Document the computer resources development strategy.
- Document the concept behind software support plans and the resources needed to make that support possible.
- Identify guidelines (for example, policy directives, instructions, and technical orders) that users managing computer software in the system may refer to for help.
- Define changes or new directives needed for operating or supporting computer software in the system.

3.10.2.3. The program manager and the parent organization will approve the CRLCMP and work with using and supporting commands before the full-scale development (FSD) phase and again before the production phase.

3.10.2.4. When unable to complete the CRLCMP during the concept exploration phase, the program manager will notify the HQ USAF office of primary responsibility through program channels before going on to the next phase. ***Note: By approving or coordinating work on the CRLCMP, all parties agree to its provisions and requirements.***

3.10.2.5. During development personnel refer to the CRLCMP to create new MAJCOM or local instructions or guidelines, or modify existing instructions or guidelines.

3.10.2.6. After the system is delivered, the operating command assumes responsibility for the CRLCMP.

3.11. Open Systems Guidelines. An open system implements sufficient standards for interfaces, services, and supporting formats to enable properly engineered application software to:

- Be ported with minimal changes across a wide range of systems.
- Interoperate with other applications on local and remote systems.
- Interact with people in a style that facilitates user portability.

3.11.1. The Air Force:

- Requires the use of open systems to make it easier to operate software on different systems.
- Builds its open systems policy on the standards for Portable Operating System Interface for Computer Environment (POSIX), Government Open Systems Interconnect Profile (GOSIP), Structured Query Language (SQL), and X-Windows.

3.11.2. Refer to:

- The National Institute for Standards and Technology (NIST) Special Publication 500-187, *Application Portability Profile (APP)*, for information about the use of the U. S. Government's open system environment (OSE) profile.
- The Defense Information Systems Agency *Corporate Information Management (CIM) Technical Reference Manual* for additional guidelines.

3.11.3. Exemptions. Guidelines in **3.11.** don't apply to:

- Computer systems that form an integral part of a weapon system and for which no OSE exists.
- Self-contained systems software (for example, automotive diagnostic systems).
- Microcomputer and workstation software developed exclusively for academic research.

3.11.4. Background:

- Refer to the NIST APP for open systems specification guidelines within all Air Force software development agencies. ***Note: All Air Force computer system software must meet certain portions of the APP.***
- Follow APP guidelines when no office has approved a waiver or exception request.

3.11.5. POSIX. All Air Force computer systems must specify POSIX when it's cost effective to do so or when a life cycle analysis of the system requires it.

- Applications software for these systems, both COTS and custom-developed, must run on a POSIX compatible operating system.
- Submit an exception request for dedicated servers (for example, data base servers) or other special-purpose hardware for which the Air Force doesn't develop software. ***Note: All other standards still apply (for example, Federal Information Processing Standards Publication {FIPS PUB} 127-1, Database Language SQL, 1990 Feb 2, specifies access by means of SQL for dedicated data base servers).***
- Move existing systems to POSIX when performing routine maintenance or modernizing software. ***Note: POSIX compatible operating systems exist for the most recently developed hardware.*** In several cases, vendors support coprocessing both in POSIX compatible and proprietary operating systems.

3.11.6. GOSIP. All Air Force computer systems must specify GOSIP when it's cost-effective to do so or when the life cycle analysis requires it. ***Note: Systems may also specify other protocols necessary to operate software within existing systems (for example, transmission control protocol/internet protocol).***

3.11.6.1. For existing systems, develop plans to change to GOSIP according to the Air Force GOSIP Transition Plan maintained by HQ AFC4A/XPS.

3.11.7. SQL:

3.11.7.1. All Air Force computer systems developed with data base management systems must specify data base management systems used and SQL (FIPS PUB 127-1). ***Note: Don't use vendor-unique extensions to the SQL standard when doing so makes it difficult to transfer or share files.***

3.11.7.2. All Ada applications must adopt the SQL Ada Module Extensions standard when systems offer it. ***Note: If Air Force products that have this feature can't be found, use vendor-supplied or locally developed Ada-SQL bindings.***

3.11.8. X-Windows. All Air Force computer systems must specify the X-Windows user interface, except as noted below.

3.11.8.1. Air Force requirements may specify a graphical user interface (GUI) tool kit. In this case, system developers will use a virtual application programming interface (VAPI) to isolate an application from the GUI to allow for software compatibility on different systems.

3.11.9. Personal Computers. To make sure computer users can freely access the personal computer market, applications developed for an MS-DOS, OS/2, Solaris, Next, or Macintosh compatible environment will comply with all other applicable open systems standards (for example, Ada, SQL, and GOSIP), and when possible, will make use of a VAPI that allows the application to be used in a POSIX/X-Windows environment.

3.11.10. Other Considerations. The APP presents guidelines on the characteristics of various software specifications by class to help users determine which specifications to use. The APP:

- Lists many interface standards that may apply to particular software systems, including data interchange standards and graphics standards.
- Presents standards, but is not itself a standard. In documentation, don't justify a proposed system by saying it "conforms to the APP." You must cite a listed standard.
- Doesn't list extensions supplied in compatible commercial products. Air Force software developers will avoid using extensions when doing so limits use of the application on different systems.

3.12. Firmware Management. Firmware combines hardware with read-only computer instructions and data on the hardware device. Manage both the software characteristics and hardware characteristics of firmware by:

- Developing, documenting, and maintaining computer firmware such as computer software configuration items (CSCI) or computer software components throughout the life of the program regardless of the software storage medium (for example, magnetic tape, magnetic disk, read-only memory, or programmable read-only memory).

- Managing and documenting firmware development equipment, read-only memory programming equipment, and read-only memory devices such as hardware configuration items or hardware components.

3.12.1. Mark devices according to local procedures.

3.12.2. Identify devices by part reference number, manufacturer's code, and a unique identifier (such as a national stock number).

3.12.3. Organizations responsible for programming read-only memory devices will:

- Maintain cross-references between the unique identifier assigned to the device for stocking and distribution and the CSCI identification used for software configuration control.
- Include the revision number of each device used in firmware configurations, read-only memory programming equipment, and other read-only memory devices to make sure parts are replaced from the same or later revision.

3.13. Software Metrics. Collect, analyze, and use software metrics throughout the software development life cycle. Acquisition Policy 93M-017, *Software Metrics Policy*, identifies the mandatory Air Force "core metrics" and additional Air Force "optional metrics" to use. Further guidance on metrics collection and use is in DoD Instruction 5000.2, Part 6, Section D, and AFP 800-48, *Software Management Indicators* (to be converted to AFPAM 33-123).

3.14. Functional Design Authority (FDA). The FDA is an individual who is normally the MAJCOM or field operating agency (FOA)senior official assigned C4 responsibilities. The FDA is the authority on the specific software and computer system support within the assigned domain. The FDA validates program funding for and oversees development and maintenance of systems and applications software for a particular function or category of activities. The FDA is the Air Force advocate for all software support requirements for users of the systems. Only one FDA is authorized for software systems support and accountability in each of nine functional domains. The FDA is designated for systems accountability containing Air Force-supported software within its community of interest; however, whenever command or functional lines are crossed, FDAs must coordinate as needed.

3.14.1. FDAs are established for software support as follows:

- Air Combat Command: Air combat systems.*
- Air Mobility Command: Air mobility systems.*
- Air Force Space Command : Space systems* and missiles.
- Air Force Materiel Command (AFMC): Wholesale logistics support systems; research and development systems and services; research, development, test, and evaluation facilities and management systems; test and evaluation support systems; ;supercomputing and scientific systems;. standard base-level data processing and information systems; standard MAJCOM-level non-C2 processing systems; and standard communications systems.
- Air Education and Training Command: Education and training systems, recruiting, and student management systems.
- Air Intelligence Agency: Intelligence systems, information warfare, and cryptological services.
- Air Force Military Personnel Center: Manpower and personnel systems and mission support for such activities.

- Air Weather Service: Weather systems and weather and space environmental product centers.
- HQ USAF/XOM: War-gaming and operational modeling and simulation systems.

* Embedded systems are the province of AFMC.

3.14.2. The FDA:

- Represents the Air Force community in matters dealing with computer systems and software engineering with Air Force, DoD, and national agencies.
- Acts as single point of contact for the Air Force community in matters dealing with computer systems and software engineering.
- Establishes standards and guidance for the Air Force community related to computer and software systems following Air Force policy and instructions.
- Establishes software development activities (SDA) when no existing central design activity (CDA) will manage development or maintenance of the software.
- Defines authority and area of responsibility for each assigned CDA or SDA.
- Implements policies, standards, and guidance for total life cycle management for designated computer and software systems.
- Provides oversight, where the thresholds to be established by AFI 33-103, *C4 Systems Requirements Development and Processing* are not exceeded, for the Air Force community to ensure compliance with public law, DoD, national agencies, and Air Force software policies and standards.

3.14.3. A CDA will:

- Represent the Air Force community on software production within DoD and national agencies.
- Serve as the single point of contact on software production authority within its domain for the Air Force.
- Establish policies, standards, and guidance for the Air Force community in software production.
- Establish an Air Force community SDA under the CDA for designated computer systems.
- Establish a core SDA to aid the CDA.
- Define the authority and the area of responsibility for each of the SDAs.
- Implement policies, standards, and guidance to fully implement the core SDA and other SDAs.
- Implement policies, standards, and guidance to total life cycle support for software systems.
- Provide oversight for the Air Force community of interest software production to ensure compliance with public law, DoD, national agencies, and Air Force software production policies and standards.
- Coordinate with other Air Force CDAs on software reuse, open systems, etc.

3.14.4. An SDA will:

- Represent the FDA on software production within specifically assigned command systems areas of responsibility.
- Act as single point of contact for software production authority within a specific area of responsibility.
- Produce software systems for specific areas of responsibility.
- Maintain software systems throughout their life cycle for a specific area of responsibility.
- Implement procedures for compliance with public law, DoD, national agencies, and Air Force software production policies, standards, and guidance.

Section C—Software Development

4. General Requirements.

4.1. Security. Most DoD software, whether part of a critical mission or AIS, requires some level of security. DoD program managers and software developers must integrate computer security into their systems using write-system software that prevents inadvertent or unauthorized access to DoD computer systems and notifies security personnel of intrusion attempts. ***Note: Refer to AFIND 5 and AFI 33-202, The Air Force Computer Security Program (will supersede AFSSIs 5100, The Air Force Computer Security Program {COMPUSEC}, 5101, Computer Security in the Air Force Acquisition System, and 5102, Computer Security for Operational Systems, when published) for more information.***

4.2. Contingency Planning. All organizations that develop software for use during contingencies must:

- Tailor software for streamlined use during contingencies and exercises by deleting or delaying unnecessary processes and reports.
- Develop easily implemented tailoring actions and automated backup procedures.
- Work with users to develop processes that convert from automated to manual processing, and back again to automated processing.
- Design systems software to operate under combat conditions without further modification.

4.3. Disaster or Emergency Planning. Organizations plan and develop all computer systems to sustain operations during disasters or emergencies. Personnel must:

- Create backup copies of all mission-critical software and store the originals in a separate location (another room or building suffices).
- Develop plans for protecting classified and sensitive unclassified information according to AFIs 31-401, *Information Security Program Management* (will supersede AFR 205-1, *Communications-Electronics {C-E} Equipment,* and AFR 205-43, *Safeguarding NATO Classified Information* {FOUO}, when published); 10-1102, *Safeguarding the Single Integrated Operational Plan (SIOP)* (will supersede AFR 205-25, {S}*Safeguarding the Single Integrated Operational Plan {SIOP},* when published); USAF Intelligence (USAFINTEL) 201-1, *The Security, Use, and Dissemination of Sensitive Compartmented Information;* and AFI 33-202.

4.4. Reliability and Maintainability (R&M). R&M ranks with saving money, meeting deadlines, and developing technical performance as one of the most important aspects of computer resources development and support. When defining computer resource requirements:

- Test built-in components, fault tolerance, field-level software reloading, and standardized maintenance interfaces.
- Use a previously tested maintenance and diagnostic system.
- Use software engineering techniques and design approaches to make software maintenance and modifications easier to do.

4.5. System Safety. Organizations must consider safety factors during systems development and:

- Develop computer resources critical to the safe operation and maintenance of the system.
- Use IV&V, simulation, and other extended testing methodologies for critical CSCIs and HWCIs in flight, nuclear, or overall safety systems.
- Refer to MIL- STD-882B, *Systems Safety*, for detailed guidelines.

4.6. Engineering Studies. Results of these studies form the basis for the computer resources areas of the system/segment specification. Personnel perform the studies listed below.

4.6.1. Studies for Analyzing Requirements and Alternatives. Personnel:

- Define exactly what the software must accomplish as well as requirements for security, software quality, and sharing data.
- Encourage the use of methods, such as reusing or sharing existing software, that don't require developing new software.

4.6.2. Studies for Refining Requirements. Personnel analyze the system requirements, including constraints, to identify driving development factors such as:

- System interfaces.
- The ways in which different systems will share software.
- Communications between systems.
- Personnel needs.
- The anticipated level and urgency of changes.
- Requirements for reliability and responsive support.

4.6.3. Studies to Define Requirements.

- Prepare a first draft of plans for allocating the requirements between hardware and software.
- Document the requirements for each software configuration item in a first draft of the software requirements specification.

4.6.4. Studies of Operational Concept Analysis.

- Analyze the operational concept to determine the role of computer resources.
- Pay particular attention to requirements for mission preparation, operator interface, system controls, and mission analysis.

4.6.5. Trade-Off and Optimization Studies.

- Determine how to work within the system constraints posed by the operations and support concepts, performance and logistical requirements, availability and maturity of technology, and limitations on cost, schedule, and resources.
- Study various computer resource approaches for meeting requirements for operational, networking, security, and support.
- Consider the suitability of standard computer languages, instruction-set architectures, and interfaces.
- Consider whether to improve support services or system performance, and whether to use existing Government resources or COTS resources, or develop new resources.

4.6.6. Feasibility Studies. Conduct feasibility studies for each approach under consideration to estimate costs and production schedules. ***Note: Feasibility studies may require personnel to develop experimental computer resources.*** In these cases, tailor the software development life cycle to accommodate program goals and constraints.

4.6.7. Risk Analysis Studies.

- Assess the risks associated with implementing different computer resources for each concept under consideration.
- Report these risks in the system-level risk management plan or in the CRLCMP.

4.6.8. Software Support Studies. Conduct software support studies to:

- Refine the system support concept and allocate software support requirements.
- Determine software identification procedures (that is, self-identification or identification plates affixed to the outside of the computer).

4.7. Requirements. Allocate requirements to CSCIs by separating application and system software.

4.7.1. The CRWG will classify each software requirement as either a mission or system function.

4.7.2. The program office will use this categorization as a guide when assigning functions to CSCIs.

4.7.3. The CRWG will further classify each CSCI as either a mission or system CSCI when software support personnel under different commands share responsibilities.

4.7.4. If personnel in the CRWG can't agree on the assignment of support responsibilities, a working group chaired by HQ USAF/XO will resolve the issue.

4.7.5. For systems that require modification in the field to keep pace with a growing threat, developers must define the content and anticipated frequency of software releases for both routine and wartime scenarios.

4.7.6. The implementing command converts these scenarios into quantitative requirements.

4.7.7. Developers perform software modification support analyses and test to make sure systems comply with requirements.

4.7.8. For programs that have a modified life cycle, the program management directive (PMD) will:

- Specify which tasks can be modified or deleted from the program.

- Correct skipped or combined phases unless directed to do otherwise in the PMD.

4.8. Design.

4.8.1. Security.

- Design C4 systems using security features already incorporated in C4 systems hardware and operating systems.
- Design additional or augmented security features only if those delivered with purchased products don't meet system security requirements.
- Design flexible applications that work with existing security features but can respond to changing needs.

4.8.2. Deployment Considerations.

4.8.2.1. Design software that keeps operator intervention to the absolute minimum.

4.8.2.2. Design retrieval procedures, when possible, that correspond to home-station processes.

- Tailor software to reduce unnecessary information in the database and in user reports.
- Design software according to DoD Instruction 5000.2/Air Force Supplement 1.
- Design software that personnel can move from one system to another with minimal or no modifications.

4.8.3. Make maximum use of existing software.

- Develop software products, whenever possible, that can be reused.
- Establish software libraries at CDA, Software Support Activities (SSA), or SDAs. Check existing libraries listed in the Air Force Reuse Implementation Plan (AFRIP) for reusable software. ***Note: The AFRIP applies to all personnel developing Air Force software, including embedded systems, command and control, and business or administrative functions.*** Each MAJCOM and FOA designates a reuse project officer responsible for identifying and procuring reusable software assets. For more information on the AFRIP, contact SSC/SSBT.

4.8.4. Portability.

- Refer to AFP 700-50, Volume. 1, for detailed information on the APP.

4.8.5. Product Improvement. Design systems to allow for growth during development, pre-planned product improvement, and modification during deployment.

4.8.5.1. The CRWG:

- Decides how much flexibility and spare capacity a system needs.
- Assesses the need for flexibility against the cost-effectiveness of providing it.
- Documents its recommendations in the CRLCMP.

4.9. Development.

4.9.1. Software Standards. Where cost-effective, use modern software development techniques to improve all areas of software performance. Examples of these techniques include:

- Fourth-generation languages and tools.

- Integrated application software development and maintenance systems.
- Data base management systems.
- Active data dictionaries.
- Graphics facilities.
- Application and procedural language interfaces.

4.9.2. Programming Languages. Air Force policy requires the use of the Ada programming language as outlined in DoD Instruction 5000.2/Air Force Supplement 1. Refer to **6.4.** for information on Ada exception requests and Ada waivers.

4.9.3. Software Tools. The STSC works for the DoD to oversee evaluation of software development tools.

4.9.3.1. All software agencies will work with the STSC to help identify effective tools.

4.9.3.2. The software development effort uses a common set of tools integrated into a software engineering environment (SEE).

4.9.3.3. The SEE includes editors, compilers, debuggers, code generators, library managers, test generators, and software configuration managers.

4.9.3.4. Use software metrics, computer-assisted software engineering, and requirements tractability tools.

4.9.4. Software Inventory. The *Computer Systems Authorization Directory (CSAD)* serves as the official catalog of Air Force authorized software systems. Systems descriptions contained in the CSAD include systems under development or in operation.

NOTE:

HQ AFC4A/XPSD can provide further information about the CSAD and its use.

4.9.5. Software Development.

4.9.5.1. Develop all software according to DoD 2167A-STD (or MIL-STD-498, pending publication).

4.9.5.2. Manage computer software development as a subordinate yet significant part of overall system development.

4.9.5.3. Develop software alongside other system components, even if it cannot be directly correlated to the other system components being developed.

- Maintain a system or subsystem perspective when not maintaining direct correlation to ensure timely and successful system integration.
- Modify and produce software during any phase of the system life cycle, even if the process spans more than one development phase.
- Modify and produce software, regardless of the length of the development phase, according to the established software development cycle.
- Develop software to conform to reviews, products, baselines, and developmental configurations established for the software development cycle.

4.9.6. Software Development Methodology. Software managers will:

- Document the process or methodology used to develop or maintain software systems within their organizations.
- Decide, at the beginning of every new development or maintenance project, on the methodology best suited to meet the project's needs.
- Develop procedures for reviewing and reporting on the use of software development techniques. As a minimum, these reviews should consider product reliability, vendor support and training, and adequacy of documentation.

4.9.6.1. HQ USAF/SC:

- Uses reports from software managers to consider adopting recommended techniques as standards.
- Monitors and reports on development efforts within the Air Force and other DoD components.

4.9.7. Development of Prototype Computer Resources. Throughout the software development life cycle, personnel may, if necessary, develop prototype system models that incorporate computer resources or prototype software that demonstrates critical algorithms, control sequences, timing, or operator interfaces.

4.9.8. Software Redevelopment. The program manager works with the supporting and operating organizations to develop new software developed during this phase to modify or enhance existing software.

4.9.8.1. Work during this phase must follow the software development cycle, tailored to accommodate production activities.

4.9.9. System Modifications and Deficiencies. Report and process requirements for changes to computer resources that affect system hardware as system modifications (DoD Instruction 5000.2/ Air Force Supplement 1) or as system deficiencies (TO 00-35D-54).

4.9.10. Software Reports and Reporting Procedures. Every organization that develops or manages software must develop procedures to track and report software failures and assess the general health of its software life cycle management program. These procedures apply to both the software development phase and software support phase of the software life cycle, and should be adhered to in both phases.

4.9.11. Software Change Frequency.

4.9.11.1. When applicable, convert group software changes into blocks to facilitate change processing.

4.9.11.2. Determine the frequency of block releases and updates by balancing the need for responsiveness with efficiency considerations.

4.9.11.3. The CRWG:

- Determines the initial frequency and schedule for software changes.
- Documents these in the CRLCMP.

4.9.12. Software Change Requests.

- Treat requirements for changes to computer resources as software change requests if they involve software and don't affect system hardware.
- If the originator can't determine whether the change would affect software only, report the requirement as either a software change request or hardware modification or deficiency.

4.9.13. Source and Justification. Requests for changes to computer software may originate from any organization that has a role in implementing, operating, using, or supporting the system.

4.9.14. Setting Priorities. The originator will suggest one of three mission-impact priorities by stamping:

4.9.14.1. EMERGENCY. If the request requires immediate resolution to prevent:

- Serious compromise of national security.
- Fatal or serious personnel injury or illness.
- Extensive loss or damage of equipment.
- A severe restriction or degradation of combat readiness.

4.9.14.2. URGENT. If the request requires prompt resolution to prevent:

- Serious degradation of deployed equipment.
- Potential injury to personnel or damage to equipment.
- Unmet program deadlines or unbudgeted costs.
- A lost opportunity for significant system life cycle cost savings.
- Degradation or loss of a security-relevant feature such as audit capability or access control.

4.9.14.3. ROUTINE to all requests that do not meet the criteria for EMERGENCY or URGENT designations.

4.9.15. Change Processing. Tailor computer software change requests, depending on the size, severity, and complexity of the change request. Process the requests by:

4.9.15.1. Screening.

4.9.15.1.1. Each configuration control board (CCB) and software configuration control sub-board (SCCSB) that processes software change requests must screen them. The configuration management plan, based on command or local regulations, will determine the formality of screening, and will depend on the complexity of the system. For further guidance on the responsibilities of the CCB and SCCSB, refer to AFR 14-1.

4.9.15.1.2. Forward computer software change requests to the screening office, where personnel will:

- Receive, log, and acknowledge the request.
- Consolidate duplicate requests.
- Arrange for analysis of the change request as described in **4.9.15.2.**
- Arrange for CCB or SCCSB review.
- Forward requests that require approval by other boards or action by other agencies.

4.9.15.2. Analyses.

4.9.15.2.1. Mission-Impact Analysis. The operating command will provide mission-impact analyses describing the potential effect of the change -- or not making the change -- on the mission. This analysis will:

- Include other mission-related effects such as procedural changes or operator retraining requirements the change would cause.
- Recommend revising the priority of the change request, if appropriate.
- Indicate, for routine changes, the priority of the requested change relative to other pending changes.

4.9.15.2.2. System Impact Analysis. The supporting command will perform a system analysis to identify relevant system impacts, including changes to associated test equipment, training devices, support equipment, or other systems. ***Note: If this analysis indicates the proposed solution would affect hardware, the CCB or SCCSB will submit the request according to DoD Instruction 5000.*** 2\Air Force Supplement 1 or notifies the originator.

4.9.15.2.3. Technical Analysis. The organization most likely to accomplish the suggested change will perform a technical analysis. ***Note: Provide other interested organizations the opportunity to conduct a technical analysis.*** When software support personnel under different commands share responsibilities, both software support organizations will perform a technical analysis to:

- Identify potential solutions.
- Estimate resources needed to accomplish the change, including personnel, time, budget, and testing requirements.
- Identify how the change would affect spare computer resources such as memory or timing.
- Assess the risk associated with making the change.
- Suggest a schedule for completing the change.

4.9.15.3. Assignment. Based on the results of the mission impact, system impact, and technical analyses, the CCB or SCCSB will evaluate, schedule, and assign approved change requests to the appropriate development organization for solution. This assignment will include a computer software distribution item (CSDI) designating the version/release/update (VRU) information for making the change.

4.9.16. Status Tracking. The CCB or SCCSB will track the development of approved software changes through installation.

4.10. Testing.

4.10.1. Test Planning. Run computer resource tests according to AFI 99-101, *Developmental Test and Evaluation* (will supersede AFR 80-14, *Test and Evaluation*, and AFR 80-19, *Support of Nongovernment Test and Evaluation*, when published).

4.10.1.1. The Test and Evaluation Master Plan (TEMP) in AFI 99-109, *Test Resource Planning* (will supersede AFR 80-14, *Test and Evaluation*, when published), gives guidelines for

testing computer resources at all levels.

4.10.1.1.1. Determine the level of stress testing required (that is, stress out-of-range, stress load, and alternative signs of stress) and specify it in the test plans.

4.10.1.2. Consider using simulation and modeling for critical requirements or when unable to test using actual system components or operational environments.

4.10.1.3. Start initial test planning for computer resources early in the program and document these plans in the TEMP.

4.10.1.4. Test software on different systems if it's designed to operate on more than one system.

4.10.1.5. Establish quantitative and demonstrable performance objectives and evaluation criteria for computer hardware and software.

4.10.1.6. Determine the system or software test approach and test tools based on how critical the project is to reduce all risk to an acceptable level.

4.10.1.7. Update the TEMP to reflect the test objectives and evaluation criteria for the computer resources in the system.

4.10.1.8. Include plans for developmental test and evaluation (DT&E) and operational test and evaluation (OT&E) of computer resources according to AFI 99-101. ***Note: OT&E must show software can be used on different systems, according to AFI 99-102, Operational Test and Evaluation (will supersede AFR 55-43, Management of Operational Test and Evaluation, and AFR 80-14, Test and Evaluation, when published).***

4.10.2. System Integration and Testing.

4.10.2.1. Successively integrate CSCIs and HWCIs and test to validate integration.

4.10.2.2. Using and supporting organizations participate in system testing.

4.10.3. DT&E. The program office will make sure personnel with software expertise are available for DT&E to provide a valid technical assessment of the system according to AFI 99-101.

4.10.4. OT&E. The program office and the supporting organization will make sure personnel with software expertise are available for OT&E to evaluate the system's operational effectiveness and suitability of computer resources, according to AFI 99- 101.

4.10.5. Compiler Testing.

4.10.5.1. The procuring organization, the designated control agent for the language, and the user of the proposed system determine whether to accept the tested compiler by:

- Using the procedures developed by the Ada Validation Office (AVO) to validate Ada compilers. All Ada compilers must have an AVO validation certificate.
- Using compiler testing for other Air Force standard programming languages to verify conformance to respective standards as they become available.

4.11. Post Development.

4.11.1. Release of Software to Agencies Outside of the Air Force. To control distribution, personnel coordinate release of software through the activity scientific and technical information office, if available, and MAJCOM.

4.11.2. Software Certification. Certify all software received from the developing agency before releasing it to the operating command for OT&E.

4.11.2.1. Develop certification criteria based on engineering data and test results to make sure new or modified software meet requirements for engineering integrity, safety, security, compatibility, support, and performance.

4.11.2.2. The operating command certifies all CSCIs before releasing software for operational use.

4.11.2.2.1. Base certification on OT&E to make sure the new or modified software is ready for operational use.

4.11.2.2.2. Operational certification gives users authority to reproduce, distribute, and install the application software and to use it in an operational system.

4.11.2.3. The operating command certifies systems to run on intersystem or network environments. ***Note: This certification represents testing that goes beyond operational certification testing governed by the rules and procedures of the intersystem or network manager.***

4.11.2.3.1. Personnel may use software certified to run on different or networked systems in the designated intersystem or network environment.

4.11.3. Production Approval. Before approving computer resources for production, personnel:

- Update the functional and allocated baselines.
- Complete the FQR.
- Establish the product baseline.
- Make sure all three baselines are under proper configuration control.
- Coordinate work on the support concept.

4.11.4. Installation. (***Note: Installation includes loading and checkout.***)

4.11.4.1. The operating command will:

- Only install software certified for operational use.
- Create an abstract for each system that describes the allowable intersystem and intrasystem hardware, software, and data configurations.
- Make sure personnel mark field loadable computer assets to show the loaded configuration.
- Load spare copies of current software in readiness spares package unless provisions exist to load these spares during deployed operations.

4.11.4.2. The supporting command will publish the system abstract and make it available to operations and maintenance personnel.

4.11.4.2.1. Operations and maintenance personnel identify operational systems software. Identification methods may include:

- Physical markings down to theshop replaceable unit level.
- Maintaining a configuration status accounting system by version and serial numbers.

4.11.5. Transition Period. During transfer of the software product and maintenance responsibility from developers to the operational community, the program manager will provide software support for fielded systems. *EXCEPTION:* No transition period will occur if the developers have already transferred software, such as mission software, to an operating command.

4.11.5.1. Responsibility for computer resources will rest with the person in charge of the system or subsystem in which resources reside, unless the CRLCMP details incremental transfer of such responsibility.

4.11.5.2. Personnel work during the transition period according to command and local regulations, as modified by the CRLCMP.

4.11.5.3. The CRLCMP outlines any special configuration management procedures required during the transition period.

4.11.6. System Management.

4.11.6.1. The implementing command manages systems through the deployment phase.

4.11.6.2. The supporting command assigns a system manager, who assumes overall program management responsibility at system delivery.

4.11.6.3. When personnel under different commands manage software support responsibilities, the CCB with primary responsibility and authority for overall configuration management of the system:

- Controls the interfaces between mission and system software.
- Oversees overall system integrity.

4.11.6.4. For systems with a significant amount of software, personnel establish one or more SCCSBs to facilitate computer software change processing.

4.11.7. Software Maintenance. For guidelines on maintaining software, refer to:

- The software maintenance cycle described in DoD 2167A-STD (or MIL-STD-498, pending publication).
- Command and local directives that specify detailed procedures for handling emergency, urgent, and routine changes.

4.11.7.1. Emergency Change Requests.

- Resolve emergency software change requests quickly.
- Do not implement a complete CSDI update only for expediency. ***Note: Personnel must conduct a CSDI update at the earliest practical time.***

4.11.7.2. Urgent Change Requests.

- Prioritize urgent software change requests.
- Develop CSDI updates when implementing an urgent software change request, or a group of simultaneous requests.

4.11.7.3. Routine Change Requests.

- Resolve routine software change requests promptly.
- Group such requests based on mission-impact analysis and level of difficulty to determine which may involve developing a CSDI update or release.

4.11.7.4. Independent Verification and Validation (IV&V). Conduct IV&V for all VRUs.

4.11.7.5. Documentation.

- Update all documentation (operator or user, maintenance, programmer, training, system or software specifications) to reflect software changes.
- Distribute updated documentation at the same time as updated CSDI products.

4.11.8. Software Distribution. The term "distribution" refers to the stage when personnel reproduce, archive, or publish software as well as the distributing software to users.

- Distribute software releases as CSDIs.
- Distribute CSDIs with changes to personnel developing user documentation.

Section D—Support

5. General Requirements.

5.1. Software Support. To make software support responsive, effective, and efficient, personnel tailor the traditional roles of the implementing, supporting, and operating commands to meet system and mission requirements. The program office will:

- Plan to buy dedicated hardware and software to aid the system under the support concept described in the CRLCMP.
- Assign overall system management responsibility and authority to a single system manager when support responsibilities fall under separate commands.

5.1.1. The system manger will control software interfaces as necessary to ensure system integrity.

5.1.2. Software support organizations will participate in development and testing.

5.2. Sharing and Redistributing Software.

- Try to meet requirements through local, MAJCOM, Air Force, or DoD sharing and redistribution programs before developing new software (for example, the *Air Force Information Resources Dictionary*).
- Develop controls to protect shared classified software. ***Note: Refer to the AFRIP for more guidelines.***
- Distribute software using distribution systems common to multiple weapons or information systems.
- Identify software according to DoD Instruction 5000.2/Air Force Supplement 1, paragraph 3.k.

5.2.1. AFMC will make its capabilities available for distribution of software and documentation to operating commands that choose to use them.

5.2.2. Operating commands use system-unique software distribution methods for responsiveness or efficiency reasons.

5.2.3. The CRWG will identify the software most likely to require special distribution and define the distribution method.

5.2.4. The CSAD:

- Supports the objectives of, and provides input to, the Federal Software Exchange Program.
- Provides a catalog of descriptions of automated data systems (ADS) operating on automated data processing equipment (ADPE) in the Air Force.
- Lists systems that can satisfy specific software requirements.
- Includes the software developed.
- Has detailed descriptions to permit the reviewer to determine whether an existing application meets requirements.
- Includes a data system designator (DSD) on any software developed, or any software acquired from another Federal agency. ***Note: Obtain the DSD from SSC/XPSD.*** For information on accessing the on-line CSAD, contact HQ AFC4A/XPSD.

5.2.4. (Added-AFMC)

- Data System Designator (DSD) action requests for AFMC are made through HQ AFMC/SCWD utilizing AF Form 1375**, Data Systems Authorization Directory (DSAD) Request**. RCS: HAF-SCX(AR)8501 applies. Samples for requesting, updating and deleting DSDs using the AF Form 1375 are contained in attachments 1 through 3.

5.2.5. Use the Federal Software Exchange Center (FSEC) when possible to reduce software development costs.

5.2.5.1. The FSEC, as part of the National Technical Information Service (NTIS) of the Department of Commerce:

- Collects and catalogs summaries of Federal agency software.
- Publishes these summaries and has them available on a subscription basis (NTIS FSEC, 5285 Port Royal Road, Springfield VA 22161).

5.2.6. Develop and execute a software sharing and support agreement with Federal activities, as necessary.

5.2.6.1. Each agreement must cover the type and scheduling of support, types of and limits on technical assistance, all reimbursable cost factors, and identified billing and financing system.

5.2.6.2. Reimbursable cost factors must include the prorated share (exclusive of military pay and allowances) of direct labor, materiel, and overhead costs to provide support, as well as full costs of dedicated support equipment or technical assistance.

5.2.6.3. Refer to AFR 177-102, *Commercial Transactions at Base Level (PA)*, for further information on agreements.

5.2.7. Obtaining Excess Air Force Software.

- Make every effort to share existing software.

- Review local, MAJCOM, USAF, and DoD redistribution programs for excess software if sharing isn't possible.

5.2.7.1. Consult:

- The *DoD Automation Excess Bulletin* for listings of excess software throughout the Federal Government.
- The Command Excess Equipment Redistribution System, available in the continental United States.
- The Defense European and Pacific Redistribution Activity Office, available overseas.
- The Air Force Software Reuse Plan for more guidelines.

5.3. Software Libraries. Set up software libraries at all development centers to catalog software for reuse locally and throughout the Air Force.

5.4. Security. Besides carefully using underlying security capabilities, personnel may consult:

- The *Information Security Products Catalog*, published annually and updated quarterly by the National Security Agency, which gives evaluation information on computer security, cryptographic, TEMPEST-tested, and destruction equipment.
- The *Air Force Assessed Products List*, available from AFIWC/EA, which gives information on computer security system and subsystem assessments requested by Air Force users.
- The Air Force Computer Emergency Response Team (AFCERT) which provides 24 hour computer security incident handling of Air Force systems. The 24-hour hotline number is 1-800-854-0187.
- AFIWC/EA provides C4 system security technical support for the complete life cycle of the system.

5.5. Software Maturity Assessment. To improve the software development and support process of Air Force software intensive systems, the Air Force established the Air Force Software Process Assessment Program. The basis for this program is the Software Engineering Institute's model on software maturity assessments, the Capability Maturity Model. Guidance concerning this program applies to all organizations that develop or maintain software.

5.5.1. Senior management of the CDAs, SSAs, and SDAs must commit to actively sponsor, support, and participate in the software process assessment program.

5.5.2. Air Force CDAs, SSAs, and SDAs with more than 10 people or a budget greater than $1 million must complete an initial software maturity assessment by 1 October 1994.

5.5.2.1. Perform follow-up assessments every two to three years (according to the SAF/AQK Action Memorandum, 23 September 1991).

5.5.2.2. A team of personnel from the assessed CDA, SSA, and SDA, and trained assessment evaluators conduct the assessment.

5.5.2.3. HQ AFC4A/XPSP:

- Serves as primary source of trained evaluators to conduct assessments.

- Generates software process improvement programs that detail their assessment services as well as their responsibilities and those of CDAs, SSAs, and SDAs. For more information contact HQ AFC4A/XPSP.

5.6. Support Resources. Support resources include personnel, facilities, hardware, and software needed to support the system being developed (dedicated) or needed to support several systems (generic).

5.6.1. Personnel identify, plan, and budget these resources early in the system development cycle.

5.6.2. When evaluating support resource alternatives, the CRWG will analyze existing software support facilities and tools for modification or upgrade.

5.6.3. The implementing command normally develops dedicated software.

5.6.4. The operating or supporting command normally arranges for generic support resources.

5.6.5. The CRLCMP identifies dedicated and generic support resource requirements, including the purpose, timing, and location of support.

5.7. Support Documentation. Support documentation includes documents relating to system management, design, operation, and maintenance.

- Deliver all software support documentation and operating details to users to permit organic government support for the life of the system.
- Deliver graphics documentation on electronic media when practical.

5.7.1. The CRLCMP will identify the major software support documents for development.

5.8. Support Methodologies. Refer to DoD 2167A-STD (see MIL-STD-498, pending publication), MIL-STD-490B, *Specification Practices*, and MIL-STD-1521B for software enhancement and modification projects covered by this instruction.

5.9. Organic Support. Base decisions to implement an organic support concept for system computer resources on the guidelines and procedures of AFI 38-203, *Commercial Activities Program* (will supersede AFR 26-1, Volume 1, *Manpower Policies and Responsibilities for the Commercial Activities Program* when published)..

5.10. Interservice Support. For programs with potential for interservice support, the CRWG will:

- Analyze interservice support alternatives along with other support concepts.
- Consider operational requirements, life cycle costs, technical capabilities, service-unique computer resource standards, and anticipated support priorities during crises.

5.11. CRWG.

- Establish a CRWG for each system using computer resources.
- Consider using an existing CRWG for modification programs and those that already exist for related ongoing programs.

5.11.1. CRWG members will actively participate in all aspects of programs involving computer resources (for example, program management reviews, design reviews, and audits).

5.11.2. The program manager, with the coordination of the operating, supporting, and participating commands, will formally charter each CRWG.

5.11.3. The CRWG. Plays a major role in the management of computer resources in the system.

5.11.4. The Program Manager. Oversees management of the system, including computer software by:

- Resolving issues the CRWG can't through program reviews, senior-level steering committees, or direct contact with command OPRs.
- Keeping the CRWG advised when the program manager doesn't implement a formal CRWG recommendation.

Section E—Responsibilities

6. HQ USAF/SC:

6.1. Establishes regulatory and policy guidelines on computer software life cycle management (HQ USAF/SCX).

6.2. Approves or denies waivers for this instruction which are considered on a case-by-case basis (HQ USAF/SCX).

6.3. Provides appropriate guidance in technical reference codes to enable developer technical solutions to conform to Air Force architecture guidelines (HQ USAF/SCT).

6.4. After review, forwards Ada exception requests and Ada waiver requests to SAF/AQK for approval.

6.5. Establishes and monitors an oversight group that oversees personnel in different agencies to identify opportunities for standardization and prevent duplication of efforts.

6.6. Appoints Air Force agencies to oversee software programs (such as metrics, tools, and software engineering principles).

6.7. Oversees DoD-wide software policy (HQ USAF/SCX).

7. Secretary of the Air Force for Acquisition (SAF/AQ):

7.1. Works with HQ USAF/SC to review users' requests for Ada waivers.

7.1.1. Forwards approved Ada waivers to the Office of the Secretary of Defense.

7.1.2. Works with HQ USAF/SC to set up waiver policies and procedures. SAF/AQ is the only Ada waiver approval authority.

7.2. Oversees DoD-wide software-acquisition policy (SAF/AQKS).

8. Major Commands:

8.1. Designate a MAJCOM C4 systems officer (CSO) to manage software life cycle issues.

8.2. Make sure software development plans include deployed software.

8.2.1. Arrange for software support at deployment locations, when needed.

8.3. Develop procedures to get microcomputer software from, and to give report resources to, the Air Force and DoD redistribution programs.

8.4. Set up procedures to facilitate software redistribution within the command and give other MAJCOMs access to excess software.

8.4.1. Refer to DoD 7950.1-M, *Defense Automation Resources Management Manual*, September 1988, and AFM 67-1, Volume 2, Part 2, *USAF Standard Base Supply System*, for guidelines.

8.5. Approve or deny requests to contract for software development.

8.5.1. Approve only if contracting saves money.

8.6. Develop software maintenance concepts.

8.7. Train personnel and develop implementation procedures before installing MAJCOM-unique software.

8.8. Set up procedures for communicating with MAJCOMs on planned software development, projects in development, and completed software projects.

8.9. Develop procedures to reduce development costs and eliminate duplication of efforts.

8.10. Identify wartime requirements and develop implementation procedures.

8.11. Prioritize software requirements and set up procedures to stop work on processing systems, or portions of systems, not required during contingencies or emergencies.

8.12. Set up a MAJCOM SCTC.

8.13. Appoint a reuse project officer and develop a software reuse implementation plan. ***Note: See Air Force Software Reuse Implementation Plan for more details.***

9. Major Command Small Computer Technical Centers (SCTC):

9.1. Help users locate and share existing microcomputer software programs by compiling a MAJCOM catalog of user-submitted programs.

9.2. Manage the General Services Administration Software Exchange Program and give guidelines to the bases.

9.2.1. Refer to DoD Instruction 7930.2, *ADP Software Exchange and Release, December 31, 1979*, and this instruction for guidelines.

9.3. Test MAJCOM-developed, user-submitted programs for possible defects.

9.3.1. Forward programs that may benefit users Air Force-wide to SSC/SSM for inclusion in the Air Force catalog.

9.4. Review COTS software used throughout the MAJCOM if it may benefit users Air Force-wide.

9.4.1. Forward applicable reviews to:

- SSC/SSM.
- The base CSCs.

9.5. Distribute information about the Air Force and MAJCOM software catalogs to bases.

10. Headquarters, Air Force Command, Control, Communications, and Computer Agency:

10.1. Maintains the *Air Force Data Dictionary* and the CSAD.

10.2. Oversees software process improvements for the Air Force and provides a trained cadre to perform software assessments.

11. Implementing Commands:

11.1. Implement this instruction in the planning, development, acquisition, turnover, and transfer stages of systems involving computer resources.

11.2. Maintain an organic capability of computer technical and managerial expertise to perform assigned responsibilities.

11.3. Standardize computer hardware and software between and within systems.

11.4. Charter and appoint a program manager to manage system development.

11.4.1. Program Managers:

11.4.1.1. Manage the development of computer resources as an integral part of overall system development.

11.4.1.2. Maintain a life cycle view of computer resources to include the impact of near-term decisions on future operational and support capabilities.

11.4.1.3. Oversee the management of computer resources in the program management plan (PMP) and the ILSP.

11.4.1.4. Work with the supporting and operating commands to incorporate their needs into the PMP, ILSP, and other supporting plans and system documents.

11.4.1.5. Charter a CRWG.

11.4.1.6. Appoint the chairperson to serve on the CRWG until system delivery.

11.4.1.7. Define relationships between the CRWG and other working groups such as the interface control working group (ICWG) and the test planning working group (TPWG).

11.4.1.8. Develop, coordinate, and update the CRLCMP with the CRWG before system delivery.

11.4.1.9. Manage development of computer resources consistent with the CRLCMP.

11.4.1.10. Identify problems in completing, coordinating, or implementing the CRLCMP through program management channels, milestone reviews, and other reviews.

12. Supporting Commands:

12.1. Implement the procedures in this instruction that address system transfer and support of computer resources.

12.2. Maintain an organic capability of computer technical and managerial expertise to perform assigned responsibilities.

12.3. Make sure personnel develop system software according to the approved software support concept.

12.4. Program for, set up, and operate computer support facilities to modify and develop computer software and integrate and maintain the total system as defined in the CRLCMP.

12.4.1. Use existing facilities when practical.

12.5. Participate as a member of the CRWG, with the implementing and operating commands, to define the software support concept and prepare, coordinate, update, and implement the CRLCMP.

12.6. Appoint a systems manager to fulfill system support responsibilities.

12.6.1. For computer resources, the systems manager:

12.6.1.1. Manages the support of computer resources.

12.6.1.2. Maintains a life cycle view of computer resources support to include the impact of near-term decisions on future operational and support capabilities.

12.6.1.3. Chairs the CRWG after system delivery.

12.6.1.4. Works with the CRWG to coordinate CRLCMP updates.

12.7. Evaluate software documentation.

12.8. Participate in:

- Major design reviews during the acquisition cycle.
- DT&E.
- OT&E.

13. Operating (Using) Commands:

13.1. Implement this instruction in areas where the turnover, operation, and maintenance of systems involve computer resources.

13.2. Manage and support mission software according to the approved software support concept.

13.3. Set up and operate computer support facilities for modifying and developing software as defined in the CRLCMP.

13.3.1. Use existing facilities when practical.

13.4. Include computer resource requirements in system requirements documents.

13.5. Work with the implementing and supporting commands as a member of the CRWG to define the software support concept and prepare, coordinate, update, and implement the CRLCMP.

13.6. Maintain an organic capability of computer technical and managerial expertise to perform assigned responsibilities.

13.7. Test and certify new and changed software before releasing it.

13.8. Participate in:

- Major design reviews during the acquisition cycle.
- DT&E.
- OT&E.

14. Other Participating Organizations:

14.1. Implement this instruction for system OT&E involving computer resources.

14.2. Provide technical and managerial OT&E experts.

14.3. Determine the scope and nature of software testing during OT&E.

14.4. Input instructions to the CRWG on the use of IV&V.

14.5. Participate as members of the CRWG through to the completion of OT&E.

14.6. When the CRWG chairperson requests it, other training or contracting organizations may participate as members of the CRWG.

15. The Computer Resources Working Group:

15.1. Advises the program or systems manager in all areas relating to the computer software support.

15.2. Writes and updates the CRLCMP throughout the program's life cycle.

15.3. Monitors the program's compliance with computer resources policy, plans, procedures, and standards.

15.4. Recommends CSCI for grouping into CSDIs and documents the recommendations in the CRLCMP.

15.5. Integrates software test activities with the overall test program through the TPWG.

15.6. Evaluates and explores overall support concepts (as defined in the MNS, PSOC, and SOC) and documents them in the CRLCMP.

15.7. Develops preliminary software allocation plans for software support responsibility.

15.8. Studies the potential for organic and contractor support and identifies candidate organizations for performing software support.

15.9. Identifies any unique requirements for software quality such as nuclear security cross-check analysis.

15.10. Identifies and prioritizes software requirements such as:

- Networking or sharing software between systems.
- Transporting systems.
- Flexibility of programs.
- Ease of use and frequency and ease of testing.
- Reusing programs.
- Maintaining operating integrity.
- Efficiency.

15.11. Assesses the need for IV&V and recommends the appropriate level, scope, and source to the program manager.

15.12. Evaluates the use of standard equipment, high-order languages, instruction-set architectures, and interfaces.

15.13. Evaluates the need for developing software tools and recommends an approach.

15.14. Addresses system and subsystem interface requirements along with the ICWG set up by the program office. ***Note: Give preference to interface standards such as MIL-STD-1553B, Multiplex Bus, and those specified in AFP 700-50, Volume 7.***

15.15. Documents the requirements for interfaces between CSCIs and other system configurations in one or more interface requirements specification.

CARL G. O'BERRY, Lt General, USAF
DCS/Command, Control, Communications, and Computers

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

DoD Instruction 5000.2/Air Force Supplement 1, *Defense Acquisition Management Policies and Procedures*, February 23, 1991, with Change 1

DoD Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988

DoD Instruction 7920.5, *Management of End-User Computing (EUC)*, March 1, 1989

DoD Instruction 7930.2, *ADP Software Exchange and Release*, December 31, 1979

DoD 7950.1-M, *Defense Automation Resources Management Manual*, September 1988

DoD 8320.1-M, *Data Administration Procedures*, September 26, 1991

DoD 8320.1-M-1 **,** *Data Element Standardization Procedures*, January 1993

DoD 2167A-STD, *Defense System Software Development*

DoD 2168-STD, *Defense System Software Quality Program*

DoD 7935A-STD, *Defense System Software Development*

AFPD 25-2, *Support Agreements*

AFPD 33-2, *C4 Systems Security*

AFI 10-601, *Mission Needs and Operational Requirements Guidance and Procedures*

AFI 10-1102, *Safeguarding the Single Integrated Operational Plan (SIOP)*(will supersede AFR 205-25,{S}*Safeguarding the Single Integrated Operational Plan {SIOP}*{U}, when published)

AFI 21-116, *Maintenance Management of Communications-Electronics* (will supersede AFR 65-1, *Communications-Electronics {C-E} Equipment*, and AFR 66-2, *Single Manager for Modification, Major Maintenance, and Test Programs on Air Force ICBM Systems*, when published)

AFI 31-401, *Information Security Program Management* (will supersede AFR 205-1, *Information Security Program Regulation* {DoD 5200.1R/Air Force Supplement 1} and AFR 205-43, *Safeguarding NATO Classified Information {FOUO}*, when published)

AFI 33-102, *C4 Systems Long Range Planning*

AFI 33-103, *C4 Systems Requirements Development and Processing*

AFI 33-110, *Air Force Data Administration Program*

AFI 33-202, *The Air Force Computer Security Program* (will supersede AFSSI 5100, *The Air Force Computer Security (COMPUSEC) Program;* AFSSI 5101, *Computer Security in the Air Force Acquisition System*; and AFSSI 5102, *Computer Security for Operational Systems*, when published)

AFI 38-203, *Commercial Activities Program* (will supersede AFR 26-1, Volume 1, *Manpower Policies and Responsibilities for the Commercial Activities Program*, when published)

AFI 60-103, *International Military Standardization Programs* (will supersede AFR 73-6, *North Atlantic Treaty Organization Military Agency for Standardization Coordinating Committee, and American-British-Canadian-Australian Armies Interational Military Standardization Programs,* when published)

AFI 99-101, *Developmental Test and Evaluation* (will supersede AFR 80-14, *Test and Ealuation,* and AFR 80-19, *Support of Nongovernment Test and Evaluation,* when published)

AFI 99-102, *Operational Test and Evaluation* (will supersede AFR 55-43, *Management of Operational Test and Evaluation,* and AFR 80-14, *Test and Evaluation,* when published)

AFI 99-109, *Test Resource Planning* (will supersede AFR 80-14, *Test and Evaluation,* when published)

AFR 14-1, *Configuration Management*

AFR 177-102, *Commercial Transactions at Base Level* (PA)

AFMAN 171-100, Volume 6, *Development and Documentation of Automated Data Systems (ADS) - Small Computer*

AFMAN 171-100, Volume 8, *Automated Data Systems (ADS) Standards on the Standard Multi-User Small Computer Requirements Contract (SMSCRC) System*

AFM 11-1, *Air Force Glossary of Standardized Terms*

AFM 67-1, Volume 2, Part 2, *USAF Standard Base Supply System*

AFM 171-100, Volume 1, *Automated Data Systems (ADS) Standards*

AFM 171-100, Volume 2, *Automated Data Systems (ADS) Standarnds - H6000 Series ADS*

AFM 171-100, Volume 5, *Automated Data Systems (ADS) Series ADP*

AFM 171-100, Volume 6, *Development and Documentation of Automated Data Systems (ADS) - Small Computer*

AFM 171-100, Volume 8, *Automated Data Systems (ADS) Standard Multiuser Small ComputerRequirements Contract (SMSCRC) System*

AFP 700-50, Volume 1, *Air Force Communications-Computer Systems Architecture*

AFP 700-50, Volume 2, *Deployable Communications-Computer System Architecture*

AFP 700-50, Volume 4, *Local Information Transfer*

AFP 700-50, Volume 5, *Long Haul Information Transfer*

AFP 700-50, Volume 6, *Integrated Systems Control*

AFP 700-50, Volume 7, *Air Force Communications-Computer Systems Architectures, Software Architecture*

AFP 800-45, *Software Independent Verification and Validation (IV&V)*

AFP 800-48, *Software Management Indicators*

AFIND 5, *Specialized Communications-Computer Systems Security Publications*

Acquisition Policy 93M-017, *Software Metrics Policy*

FIPS PUB 21-1, *Common Business Oriented Language*

FIPS PUB 127-1, *Database Language SQL,* 1990 Feb 2

Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms*

MIL-STD-483A, *Configuration Management Practices*

MIL-STD-490B, *Specification Practices*

MIL-STD-882B, *Systems Safety*

MIL-STD-973, *Configuration Management*

MIL-STD-1521B, *Technical Reviews and Audits for Systems, Equipment, and Computer Software*

MIL-STD-1553B, *Multiplex Bus*

NIST Special 500-187, *Application Portability Profile (APP)*

USAFINTEL 201-1, *The Security, Use, and Dissemination of Sensitive Compartmented Information*

Abbreviations and Acronyms

ADP—Automated Data Processing

ADPE—Automated Data Processing Equipment

ADS—Automated Data System

AFC4A—Air Force Command, Control, Communications, and Computer Agency

AFCERT—Air Force Computer Emergency Response Team

AFI—Air Force Instruction

AFIND—Air Force Index

AFIWC—Air Force Information Warfare Center

AFM—Air Force Manual (old publication)

AFMAN—Air Force Manual (new publication)

AFMC—Air Force Materiel Command

AFP—Air Force Pamphlet

AFPD—Air Force Policy Directive

AFR—Air Force Regulation

AFRIP—Air Force Reuse Implementation Plan

AFSSI/AFSSM—Air Force Systems Security Instruction or Memorandum

AIS—Automated Information System

ANSI—American National Standards Institute

APP—Application Portability Profile

AVO—Ada Validation Office

C4—Command, Control, Communications, and Computer

CCB—Configuration Control Board

CDA—Central Design Activity

COTS—Commercial Off-the-Shelf

CRLCMP—Computer Resources Life Cycle Management Plan

CRWG—Computer Resources Working Group

CSAD—Computer Systems Authorization Directory

CSCI—Computer Software Configuration Item

CSDI—Computer Software Distribution Item

CSO—C4 Systems Officer

CSRB—C4 Systems Requirements Board

DoD—Department of Defense

DSD—Data System Designator

DT&E—Developmental Test and Evaluation

FDA—Functional Design Authority

FIPS—Federal Information Processing Standard

FOA—Field Operating Agency

FQR—Formal Qualification Review

FSEC—Federal Software Exchange Center

GOSIP—Government Open Systems Interconnect Profile

GUI—Graphical User Interface

HQ USAF—Headquarters, United States Air Force

ICWG—Interface Control Working Group

ILSP—Integrated Logistics Support Plan

IV&V—Independent Verification and Validation

LSA—Logistics Support Analysis

MAJCOM—Major Command

MIL—Military

MIL-STD—Military Standard

MNS—Mission Need Statement

NATO—North Atlantic Treaty Organization

NIST—National Institute for Standards and Technology

NTIS—National Technical Information Service

ORD—Operational Requirements Document

OSE—Open System Environment

OT&E—Operational Test & Evaluation

PMD—Program Management Directive

PMP—Program Management Plan

POSIX—Portable Operating System Interface for Computer Environment

PSOC—Preliminary System Operations Concept

R&M—Reliability & Maintainability

SAF/AQ—Secretary of the Air Force for Acquisition

SCCSB—Software Configuration Control Sub-Board

SCTC—Small Computer Technical Center

SDA—Software Development Activity

SDR—System Design Review

SEE—Software Engineering Environment

SMSCRC—Standard Multi-user Small Computer Requirements Contract

SOC—Systems Operations Concept

SQL—Structured Query Language

SSA—Software Support Activity

SSC—Standard Systems Center

STD—Standard

STSC—Software Technology Support Center

TEMP—Test and Evaluation Master Plan

TPWG—Test Planning Working Group

USAFINTEL—USAF Intelligence

VAPI—Virtual Application Programming Interface

VRU—Version/Release/Update

Terms

Air Force C4 Systems Architectures—A family of documents providing the specific technical framework (standards, protocols, etc.) to shape the evolution of Air Force C4 systems. (See AFI 33-101, *Command, Control, Communications, and Computer Systems Management Guidance and Responsibilities*.)

Application Software—Mission support or mission specific software programs designed by, or for, system users and customers. By using available computer system equipment and operating system

software, application software completes specific, mission-oriented tasks, jobs, or functions. It can be either general-purpose packages, such as demand deposit accounting, payroll, machine tool control, or specific application programs tailored to complete a single or limited number of user functions.

Automated Data Processing (ADP) Equipment Custodian (EC)—An individual, appointed by the commander, who works with the base Equipment Control Officer (ECO) to account for computers. Other duties may include processing orders, requesting maintenance, and duties determined by the organization commander or designated authority.

Certification—For purposes of this instruction, the act of determining that software performs without defects and viruses, and does what the supporting documentation says it will do.

Commercial Off-the-Shelf (COTS) Software—Software developed, tested, and sold by commercial companies to the general public. Examples include word processing, graphics, communications, and training software.

Command, Control, Communications, Computer (C4) Systems—Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control, through all phases of the operational continuum. (See Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms.*)

C4 Systems Officer (CSO)—At , the commander of the communications unit responsible for carrying out base communications-computer systems responsibilities. At major commands (MAJCOM), the person designated by the MAJCOM commander responsible for overall management of communications-computer systems budgeted and funded by the MAJCOM. HQ USAF/SCM is the Air Force CSO (when standard systems are under deliberation by the HQ USAF CSRB (Communications-Computer Systems Requirements Board); the 7th Communications Group commander is designated Air Staff CSO for Pentagon requirements. (See AFMAN 33-271)

C4 Technology Validation Office (Barksdale AFB LA)—The Air Force base designated by HQ USAF/SC to create models or prototypes of new C4 technologies, experiment with new policies and procedures, and test current and planned Air Force C4 systems.

Department of Defense (DoD) Redistribution Program—A worldwide, DoD program for reporting, screening, redistributing, and disposing of automation resources that prove not to be needed to run the application for which it was initially approved and acquired. (See DoD 7950. 1-M.)

Documentation—Instructions, checklists, sample printouts, and similar material that explains how to use software and hardware.

Electronics Bulletin Board—A system that connects users and a common computer host. Used to exchange software programs, technical information, and other information and data. (See AFM 11-1, *Air Force Glossary of Standardized Terms*.)

End-User—The individual who operates the computer. (DoD Instruction 7920.5, *Management of End-User Computing {EUC}*, 1 March 1989). The preferred term in the Air Force is "user."

Hardware—The physical equipment and devices forming a computer and peripheral components.

Host MAJCOM—The MAJCOM with jurisdiction over an installation and other real property, including use rights, such as leases, permits, easements, and licenses. (See AFPD 25-2, *Support Agreements*.)

Interoperability—The condition wherein different systems can operate the same software, or users

exchange information through a network. Define the degree of interoperability when referring to specific cases. (See JP 1-02.)

Life-Cycle Cost—The total cost to the government for a system over its full life, including the cost of development, procurement, operation, support, and disposal. (See AFM 11-1.)

Life-Cycle Management—The management of a system or an item, starting with the planning process and continuing through the systems' life-cycle phases (numbered 0-5) and milestones (numbered 0-5), until personnel dispose of it.

Maintenance—Any job that can be described as one that eliminates faults or keeps hardware or software running in satisfactory working condition falls into the maintenance category. (See AFI 21-116, *Maintenance Management of Communications-Electronics* {will supersede AFR 65-1, *Communications-Electronics [C-E] Equipment*, and AFR 66-2, *Single Manager for Modification, Major Maintenance, and Test Programs on Air Force ICBM Systems*, when published}.)

MAJCOM-Unique C4 system—A C4 system used by or within one MAJCOM only.

Microcomputer—This instruction refers to any small computer as a microcomputer. These include data processing systems that execute various programs. A small computer normally consists of an input device (for example, keyboard, touch screen, mouse, or scanner), peripheral storage, a visual display, a printer, and a central processing unit (CPU) with random-access and read-only memory. A small computer can operate "stand-alone" or be networked with other computers. Examples include personal computers, microcomputers, minicomputers, multi-user systems, all Standard Multi-user Small Computer Requirements contract (SMSCRC) systems, file servers, text processors, word processors, workstations, and por table computers.

Network—Two or more computers connected to each other through a multi-user system or by another electronic means, to exchange information or share computer hardware or software.

Parent MAJCOM—The MAJCOM to which an organization reports. A MAJCOM may serve as both a parent MAJCOM and a "host MAJCOM".

Protocol—A set of rules and formats, semantic and syntactic, that permits entities to exchange information. (See AFMAN 33-270.)

Public Domain Software—Software distributed without charge. Such software commonly does not have security protection features and is more susceptible to viruses. (See AFMAN 33-270.)

Requirement—A need for a new or improved information processing capability that, when satisfied, will increase the probability of operational mission success or a decrease in the cost of mission support. (See AFI 33-103.)

Requirements Contract—A delivery contract with an organization to fill orders for specific supplies or services, as needed, during a defined period, with deliveries scheduled when orders are placed.

Requirements Document—A document prepared by the respective using command that describes pertinent quantitative and qualitative performance, operation, and support parameters, characteristics, and requirements for a specific candidate weapon system. It has a mandatory attachment called the requirements correlation matrix. (See AFI 10-601.)

Resources—Used in this instruction to mean any computer, its component hardware and software, contractual services, personnel, supplies, and funds.

Risk Assessment—Process of analyzing threats to and vulnerabilities of an information system, and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost effective measures. (See AFMAN 33-270.)

Shareware—Privately or commercially-developed software that users receive free of charge but pay a fee for continued or extended use. Normally, implied or promised support by the author is minimal or nonexistent. (See AFM 11-1.)

Site-License Agreement—A contractual agreement with a commercial software company allowing the Air Force to use of their product at a specific site or by a specific group of users. Contracts typically provide free or inexpensive upgrades and allow multiple users to share software for less than it would cost to buy individual copies.

Small Computer Support Center (SCSC)—The center that oversees small computer support, normally part of the base communications organization.

Small Computer Technical Center (SCTC)—The MAJCOM center that oversees small computers technical issues.

Software—A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system, e.g., compilers, library routines, manuals, and circuit diagrams. (See JP 1-02.)

Standard C4 System—A C4 system used by more than one MAJCOM, requiring centralized oversight in planning, requirements processing, acquisition program management, and operations management. HQ USAF CSRB formally designates proposed C4 systems "standard systems."

System—For purposes of this instruction, a computer, including external peripherals and software.

TEMPEST—An unclassified term referring to technical investigations for compromising emanations from electrically operated information processing equipment; these investigations are conducted in support of emanations and emissions security. (See JP 1-02.)

User—See end-user.

Using Organization—The organization that operates and manages a computer system.

Validated Software—See Certification.

Attachment 2

KEY ORGANIZATIONS

Air Force ADPE Redistribution Program Office
7CG/GADE
1600 Pentagon
Washington DC 20030-1600
DSN: 227-5897 FAX: 224-4156
DDN E-Mail: gates@gad3b2.hq.af.mil

Air Force Information Warfare Center (AFIWC)
AFIWC/EA
250 Hall Blvd., Ste 139
Kelly AFB TX 78243-7063
DSN: 969-3167 Comm (210) 977-3167
24 Hour Security Incident Reporting Hotline: 800-854-0187
Security Bulletin Board: afcert@afiwc01.af.mil

Software Process Improvement Division
AFC4A/XPSP
203 W. Losey St., Room 1065
Scott AFB IL 62225-5224
DSN: 576-5697 FAX: 576-2874

Data Administration Division
AFC4A/XPSD
203 W. Losey St., Room 1065
Scott AFB IL 62225-5224
DSN: 576-5697 FAX: 576-2874

Standard Systems Center
SSC/SSMC
85 Hodges Avenue South
Maxwell AFB Gunter Annex, AL 36114-3218
DSN: 596-3473 FAX: 596-3262
DDN E-Mail: afscoaso@gunter-adam.af.mil
Bulletin Board: DSN 596-5471 through 5476

Documentation Standards
Standard Systems Center
SSC/XPT
200 East Moore Dr., Bldg 888
Maxwell AFB, Gunter Annex. AL 36114-3004
DSN: 596-4843 FAX: 596-4668
DDN E-Mail: root@192.31.100.148

Attachment 3

AIR FORCE STANDARD PROGRAMMING LANGUAGES

A3.1. Standard High-Order Programming Languages:

A3.1.1. Ada - Ada Programming Language, American National Standards Institute (ANSI)/ MIL-STD-1815.

A3.1.2. COBOL - American National Standard COBOL, X3.23-1974. COBOL specifications will reference:

- FIPS PUB 21-1, *Common Business Oriented Language.*
- COBOL interpretations numbers 1 through 7.
- Change 3 (with ANSI Y3.23) when a job requires the complete set of capabilities.

A3.1.2.1. When a job doesn't require the complete set of capabilities, specifications may cite subsets as reflected in FIPS PUB 21-1. (For example, the low level capability would be specified as "Low Level Subset, FIPS PUB 21-1.")

A3.1.3. FORTRAN - Refer to:

- The American National Standard FORTRAN X3.9-1978.
- MIL-STD-1753, *FORTRAN*.
- DoD Supplement to American National Standard X3.9-1978 (DoD Supplement).
- If you don't require the capabilities of MIL- STD-1753, you may use X3.9-1978 as the sole specification.

A3.1.4. JOVIAL (J73) - MIL-STD-1589C, *JOVIAL (J73) (USAF)*.

A3.2. Previous Standard High-Order Programming Languages. The Air Force will continue to use compilers acquired before the adoption of current standards until personnel approve requests for replacing equipment, until requirements dictate the acquisition of new compilers, or until personnel approve requests to substantially reimplement or redesign the system. The old standards include the following:

- **COBOL** - American National Standard COBOL X3.23-1968.
- **FORTRAN** - American National Standard FORTRAN X3.9-1966 or X3.10-1976.
- **JOVIAL** - Military Standard JOVIAL (J3) 1589C (USAF.
- **PL/1** - American National Standard Programming Language PL/1 X3.53-1976.

A3.3. Specialized Programming Languages:

A3.3.1. End-User Computing:

- **BASIC** - American National Standard--FIPS PUB 68 Minimal BASIC with ANSI X3.60-1978.
- **PASCAL** - American National Standard for PASCAL ANSI/IEEE 770X3.97-1983.

A3.3.2. Dedicated Communications Equipment:

- C Programming Language.

- Assembly Language.

A3.3.3. Hospital and Medical Applications:

- MUMPS programming language, ANSI X11.1-1983.

A3.3.4. Automatic Test Applications:

- **ATLAS** - ATLAS Test Language, ANSI/IEEE 416-1980.
- **C/ATLAS** - C/ATLAS Test Language, IEEE 716-1982.
- **C/ATLAS** - Syntax, IEEE 717-1982.

A3.4. Fourth-Generation Languages and Tools (application oriented). The types of languages and tools used for standardization are:

- Data base query.
- Decision support systems.
- Application generators.
- Report generators.
- Screen generators for visual displays.

Attachment 4 (Added-AFMC)

REQUESTING A DATA SYSTEM DESIGNATOR

SECTION BLOCK	ITEM	ACTION TO BE TAKEN
	DATE PREPARED	Enter date form was prepared
	TO	AFMC CSO/SCMD 4225 Logistics Ave., Ste 18 Wright-Patterson AFB, OH 45433-5757
	FROM	Enter office symbol and address of POC who signs form in section III as POC.
SECTION I	ACTION REQUESTED	
1	ESTABLISH DESCRIPTION	Place an "X" in this block if establishing a new DSD description.
4	INITIAL ASSIGNMENT	Place an "X" in the DSD block.
SECTION II	DESCRIPTION	
5	DATA SYSTEM DESIGNATOR (DSD)	If requesting a specific DSD number, the word "requested" must be in parentheses after the DSD number.
7	TITLE	Enter the title of the system. Do not include slashes, dashes, or parentheses between words. Do not include acronyms.
7a	ACRONYM	Should be unique.
7c	CRITICALITY	Enter criticality code (group number) of data and application. See note below.
8	ADPE	Enter type of equipment the system is to be processed on.

9	TYPE AUTOMATED DATA SYSTEM	1. Check “Air Force Standard” block if system is used by two or more MAJCOMs. 2. Check “Command Unique” block if system is used by two or more bases within a MAJCOM (nonstandard system) 3. Check “Base Unique” block if system is used by only one base. 4. Check “WWMCCS Standard” block if system is designated as such. 5. Check “Multi-Service” block if system is used by more then one DoD agency. 6. Check “Other” block if system is not one of the five types, and provide brief explanation.
10	RESPONSIBLE OFFICES	
10c	ADS MANAGER	Enter the functional OPR’s name, office symbol, and phone number. Have functional OPR sign.
10d	DEVELOPMENT CENTER	Enter development center’s name, office symbol, and telephone number.
11	OTHER INTERFACING SYSTEMS	List sequentially, all the DSDs for systems that will provide or receive data from this system.
12	DOCUMENTATION REFERENCES	

12a	COMPUTER OPERATIONS MANUAL	Enter the manual number for the system. This can be an Air Force manual, office instruction, or vendor supplied documentation. If a number has not been assigned, enter a subject series.
12b	USERS MANUAL	Enter the users manual number for the system. If a number has not been assigned, enter the subject series.
12c	IMPLEMENTATION DATE	Enter actual or anticipated date of implementation.
	TOTAL	Enter total of estimated and actual costs.
17	AUTHORIZING DIRECTIVE	Enter the document and date which approved the requirement for this system and enter the applicable directives (CSRD, PMD, PAD, etc.).
18	FUNCTIONAL DESCRIPTION	Enter a summary description of the function which has been automated. This description will not include how the function was automated. It will be from a functional user's viewpoint and not contain the workings of the system in data automation terminology. Do not include the information which has been provided in any item above.
19	RESEARCH RESULTS	Enter the DSAD or software directories which were reviewed in search of a similar system to fulfill the requirement (CDRS, CSAD, DIST, etc..).

	CONCURRENCES	
	CONCUR/NONCONCUR	Check “Concur” or “Non-concur” as appropriate.
	POINT OF CONTACT	Type name, grade, organization, office symbol, and telephone number of the system’s functional OPR or POC. Functional OPR/POC signs.
	STANDARD MANAGER	Leave blank.

NOTE:

CRITICALITY CODES (AFMAN 10-401, dated 28 Oct 1994)

Group 1--Mission Critical. The lost of these critical functions would cause immediate stoppage of direct mission support of wartime operations.

Group 2--Mission Essential. The loss of these areas would reduce operation capability because of loss of equipment or parts. If not corrected, degradation eventually causes loss of mission capability.

Group 3--Mission Impaired. The loss of these functions would not have an immediate effect on direct mission support of wartime operations.

Group 4--Nonmission Essential. The loss of these functions would have no effect on mission operations.

Group 5--Unassessable. Effect on the mission cannot be judged and falls into other groups when additional information becomes available.

Attachment 5 (Added-AFMC)

UPDATING A DATA SYSTEM DESIGNATOR

SECTION BLOCK	ITEM	ACTION TO BE TAKEN
	DATE PREPARED	Enter date form was prepared
	TO	AFMC CSO/SCMD 4225 Logistics Ave., Ste 18 Wright-Patterson AFB, OH 45433-5757
	FROM	Enter office symbol and address of POC who signs form in section III as POC
SECTION I	ACTION REQUESTED	
2	UPDATE DESCRIPTION	Place an "X" in this block if updating portions of a previously established DSD description. Enter the updated information on the request form for items that have been changed.
SECTION II	DESCRIPTION	
5	DATA SYSTEM DESIGNATOR (DSD)	Enter DSD number.
7	TITLE	Enter the title of the system. Do not include slashes, dashes, or parentheses between words. Do not include acronyms.
7a	ACRONYM	Should be unique.
10	RESPONSIBLE OFFICES	
10c	ADS MANAGER	Enter the functional OPR's name, office symbol, and phone number. Have functional OPR sign.
SECTION III	CONCURRENCES	
	CONCUR/NONCONCUR	Check "Concur" or "Nonconcur" as appropriate.
	POINT OF CONTACT	Type name, grade, organization, office symbol, and telephone number of the system's functional OPR or POC. Functional OPR/POC signs.
	STANDARD MANAGER	Leave blank

Attachment 6 (Added-AFMC)

DELETING A DATA SYSTEM DESIGNATOR

	DATE PREPARED	Enter date form was prepared
	TO	AFMC CSO/SCMD 4225 Logistics Ave., Ste 18 Wright-Patterson AFB, OH 45433-5757
	FROM	Enter office symbol and address of POC who signs form in section III as POC
SECTION I	ACTION REQUESTED	
3	DELETE DESCRIPTION	Place an “X” in this block if deleting a DSD description.
SECTION II	DESCRIPTION	
5	DATA SYSTEM DESIGNATOR (DSD)	Enter DSD number.
7	TITLE	Enter the title of the system. Do not include slashes, dashes, or parentheses between words. Do not include acronyms.
7a	ACRONYM	Enter the Acronym.
10	RESPONSIBLE OFFICES	
10c	ADS MANAGER	Enter the functional OPR’s name, office symbol, and phone number. Have functional OPR sign.
SECTION III	CONCURRENCES	
	CONCUR/NONCONCUR	Check “Concur” or “Nonconcur” as appropriate.
	POINT OF CONTACT	Type name, grade, organization, office symbol, and telephone number of the system’s functional OPR or POC. Functional OPR/POC signs.
	STANDARD MANAGER	Leave blank.